BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 60 406.1
Anmeldetag:	16. Dezember 2002
Anmelder/Inhaber:	Francotyp-Postalia AG & Co KG, Birkenwerder/DE
Bezeichnung:	Verfahren und Anordnung zur unterschiedlichen Erzeugung kryptographischer Sicherungen von Mitteilungen in einem Hostgerät
IPC:	H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 1. September 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Letang

A 9161
03/00
EDV-L

05.08.03

Francotyp-Postalia AG & Co.KG
Triftweg 21 - 26
16547 Birkenwerder

12. Dezember 2002

3207-DE

Verfahren und Anordnung zur unterschiedlichen Erzeugung kryptographischer Sicherungen von Mitteilungen einem Hostgerät

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Anordnung zur unterschiedlichen Erzeugung kryptographischer Sicherungen von Mitteilungen in einem Hostgerät, gemäß des Oberbegriffs des Anspruchs 1 und 5. Die Erfindung ist für Postverarbeitungsgeräte mit einem Sicherheitsmodul geeignet, welches eine entsprechende kryptographischen Sicherung unterschiedlich in Abhängigkeit vom einem im Postverarbeitungsgerät eingestellten Mitteilungstyp erzeugt. Sie kommt insbesondere in Frankiermaschinen, Adressiermaschinen und anderen Postverarbeitungsgeräten zum Einsatz.

Ein Frankierabdruck beinhaltet eine Mitteilung mit einer zuvor eingegebenen und gespeicherten postalische Information einschließlich der Postgebührendaten zur Beförderung des Briefes. Moderne Frankiermaschinen ermöglichen einen Abdruck einer speziellen Markierung zusätzlich zu der vorgenannten Mitteilung. Beispielsweise wird aus der vorgenannten Mitteilung ein Message Authentication Code erzeugt und dann ein Barcode als Markierung gebildet. Wenn ein Sicherheitsabdruck mit einer solchen Markierung gedruckt wird, ermöglicht das eine Nachprüfung der Echtheit des Sicherheitsabdruckes beispielsweise im Postamt (US 5.953.426).

Die Frankiermaschine JetMail® der Anmelderin ist mit einer Base und mit einem abnehmbaren Meter ausgestattet. Letzteres beinhaltet ein Sicherheitsmodul, das beispielsweise eine digitale Signatur für einen Sicherheitsabdruck der Frankiermaschine erzeugt (US 6.041.704).

Es ist außerdem bekannt, den Datenaustausch zwischen einer Frankiermaschine und einer entfernten Datenzentrale kryptographisch abzusichern, wenn ein Guthabenwert nachgeladen wird. Ein Sicherheitsmodul kann eine Hardware-Abrecheneinheit und eine Einheit zum Absichern des Druckens der Postgebührendaten aufweisen (EP 789 333 A2). Die Hardwareabrecheneinheit wurde mit einem Anwenderschaltkreis ASIC und die andere Einheit mit einem OTP-Prozessor (One Time Programmable) realisiert. Somit kann der Abrechenvorgang nicht durch eine Programmänderung manipuliert werden und außerdem kann ein beliebiger kryptografischer Algorithmus im Festwertspeicher für den OTP-Prozessor aufrufbar gespeichert werden. Ein interner OTP-Speicher speichert auslesesicher sensible Daten (u.a. kryptografische Schlüssel), die beispielsweise zum Nachladen eines Guthabens oder zum Erzeugen einer kryptographischen Sicherung einer Mitteilung der Frankiermaschine erforderlich sind. Somit kann ein bekannter Verschlüsselungsalgorithmus, beispielsweise Data Encryption Standard (DES) für die Bildung von MAC´s für Mitteilungen von unterschiedlichen Typus eingesetzt werden, wobei für jeden Typus ein vorbestimmter kryptografischer Schlüssel vereinbart wird. Ein Sicherheitsgehäuse des Sicherheitsmoduls bietet einen äußeren Schutz vor Ausspähung der kryptografischen Schlüssel (DE 201 12 350 U1).

Frankiermaschinen werden meist nur für einen einzigen Zweck entwickelt, nämlich postalische Freistempel zu drucken. Dabei kommt teuere Crypotechnologie zum Einsatz. Gelänge es, weitere Anwendungsmöglichkeiten zu erschließen, wobei die zugelassenen Signieralgorithmen verwendet werden, ohne dass eine Verwechselungsgefahr mit dem postalischen Freistempel besteht, würde das die Funktionalität des Gerätes erweitern.

Im Patent US 6058384 mit dem Titel: Method for Removing Funds from a Postal Security Device wurde bereits vorgeschlagen, eine Signatur für einen Nachladefreistempel (Refund Indicium) zu erzeugen, wobei ein

ungültiger ZIP code verwendet wird, zum Beispiel 00000-0000. Dies soll verhindern, dass ein betrügerischer Benutzer die Signatur boshaft für einen gewöhnlichen Freistempel zum Postversand verwendet.

Ein anderer Weg, die zur Verarbeitung mit dem kryptografischen Algorithmus herangezogenen Daten abhängig vom Mitteilungstyp in einer speziellen Weise zusammenzustellen oder indem das Nachrichtenformat für einen Nachladefreistempel anders gewählt wird, als das Nachrichtenformat eines gewöhnlichen Freistempels, beispielsweise ganz ohne ZIP, etc., ist aufgrund der sehr unterschiedlichen Bestimmungen der nationalen Postbehörden oder privaten Postbeförderer nicht immer gangbar.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Anordnung zur unterschiedlichen Erzeugung kryptographischer Sicherungen von Mitteilungen in einem Hostgerät zu entwickeln, wobei die unterschiedliche Erzeugung in Abhängigkeit von einem jeweils eingestellten Mitteilungstyp gesteuert wird.

Die Aufgabe wird mit den Merkmalen des Verfahrens nach dem Anspruch 1 und mit den Merkmalen der Anordnung nach dem Anspruch 5 gelöst.

Zur kryptographischen Sicherung einer Mitteilung wird eine Signatur eingesetzt, wobei sich die Signaturen in der Art ihrer Erzeugung unterscheiden, wenn Mitteilungen für verschiedene Zwecke benutzt werden. Die kryptographischen Algorithmen zur Erzeugung von Signaturen können separat oder gemeinsam in einer Logik hardwaregemäß oder programmgemäß im Festwertspeicher eines postalischen Sicherheitsgerätes PSD implementiert sein.
Ausgehend von der Überlegung, dass die Speicherung von unterschiedlichen Programmen im vorgenannten Festwertspeicher, wobei jedes Programm zur Ausführung eines bestimmten kryptographischen Algorithmuses dient, eine beliebige Kombination von Signieralgorithmen und Hashalgorithmen für einen Mitteilungstyp ermöglicht, wird eine Logik zusätzlich an ein postalischen Sicherheitsgerät angeschlossen. Die Logik führt allein oder in Verbindung mit Programmen im Festwertspeicher des postalischen Sicherheitsgerätes und gegebenenfalls zusätzlich mit Programmen im Festwertspeicher des Hostgerätes mindestens einen bestimmten

Algorithmus aus der Vielzahl der kryptographischen Algorithmen aus, wobei die Ausführung in Abhängigkeit von einem jeweils eingestellten Mitteilungstyp gesteuert wird.
Die Cryptologik weist ausgangsseitig mindestens einen Ausgang auf, der direkt oder indirekt auf den Eingang einer zweiten Logikschaltung im Inneren des postalischen Sicherheitsgerätes geschaltet ist. Die Cryptoalgorithmen können außerhalb des PSD´s in der Cryptologik und/oder innerhalb des PSD´s implementiert sein. Durch Umschalter können die Ein- oder Ausgänge von Logikschaltungen oder Parameter von Hashfunktionen von einer Logikschaltung geschaltet werden, wobei die Logikschaltungen gleich und unterschiedlich aufgebaute Cryptoalgorithmen verwenden. Ein Umschalter kann im PSD und/oder außerhalb des PSD´s implementiert sein und dabei vom PSD oder Host getriggert werden. Je weniger die Host application und je mehr die PSD application das Erzeugen einer Signatur bestimmen soll, um so geeigneter sind Varianten, in welchen der Umschalter im PSD realisiert ist. Soll im anderen Fall die Host application die Entscheidung treffen, um so geeigneter sind Varianten, in welchen der Umschalter außerhalb des PSD realisiert ist. Damit ergeben sich eine Vielzahl an Varianten der im Inneren der Cryptologik und des PSD´s implementierten Struktur bzw. der betriebsmäßigen Zusammenschaltung beider, so dass Signaturen erzeugt werden können, die für das Frankieren von Post ungültig aber für andere Zwecke geeignet bzw. gültig sind. Weitere Anwendungsmöglichkeiten im Bereich der Postbearbeitung sind noch spezielle Freistempel wie zum Beispiel postage correction indicia, oder military mail oder embassy mail. Darueber hinaus gibt es nichtpostalische Anwendungen im Bereich Ticketing und wertbehafteter Belege, für die nun sinnvollerweise dieselben zugelassenen Signieralgorithmen verwenden werden, ohne eine Verwechselungsgefahr mit postalischen Freistempel. Das gestattet es weitere Anwendungsmöglichkeiten zu erschließen, was die Funktionalität beispielsweise von Frankiermaschinen erweitert.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, vereinfachte Darstellung der Generierung einer Signatur mittels eines bekannten postalischen Sicherheitsgerätes (priort art),

Figur 2, Host-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes (Variante 1),

Figur 3, 4, Darstellung der Strukturen eines Cryptoalgorithmus,

Figur 5a, zweite Variante einer host-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes,

Figur 5b, PSD-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes (Variante 1),

Figur 6, zweite Variante einer PSD-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes,

Figur 7, dritte Variante einer PSD-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes,

Figur 8, dritte Variante einer host-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes,

Figur 9, vierte Variante einer host-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes,

Figur 10, Host- und PSD-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes,

Figur 11, Blockschaltung eines Hostgerätes.

Die Figur 1 zeigt eine vereinfachte Darstellung der Generierung einer Signatur mittels eines bekannten postalischen Sicherheitsgerätes (PSD). Über einen Eingang e des PSD 10 liegt eine Mitteilung m an einer ersten Logikschaltung 11 an, die auf die Mitteilung m einen ersten Cryptoalgorithmus anwendet. Der Ausgang a der ersten Logikschaltung 11 liegt am Eingang einer zweiten Logikschaltung 12 an, die einen digitalen Signaturalgorithmus (DAS) auf das Ausgangssignal a anwendet, um Daten für eine Signatur zu erzeugen. Die Logikschaltungen können einen Software- oder Hardwaremodul beinhalten, der den entsprechenden Algorithmus software- oder hardwaremäßig ausführt. Beispielsweise wird der aus dem US 5,231,668 bekannte Digital Signatur Algorithmus (DAS) oder ein vergleichbarer Standardalgorithmus softwaremäßig durch die zweite Logikschaltung ausgeführt. Ein entsprechendes durch einen Mikroprozessor (nicht gezeigt) abarbeitbares Programm ist im Festwertspeicher (nicht gezeigt) der zweiten Logikschaltung des Sicherheitsmoduls implementiert. Der ersten Cryptolalgorithmus wird nun im Unterschied zur bekannten Variante hardwaremäßig und extern des PSD 10 mittels der ersten Logikschaltung ausführt. In einer ersten Variante wird die ersten Logikschaltung zuschaltbar realisiert. Um Signaturen für unterschiedliche Zwecke zu generieren, wurde eine Anordnung geschaffen, die zwei verschiedene zugelassene Hashfunktionen bei demselben Signieralgorithmus benutzt.

Die Figur 2 zeigt eine host-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes. In dieser ersten Variante sind die Logikschaltung 21 für den Cryptoalgorithmus 1 und die Logikschaltung 22 für den Cryptoalgorithmus 2 eingangsseitig verbunden und führen ausgangsseitig jeweils auf Kontakte I und II eines Umschalters 24, wobei letzterer ausgangsseitig am Eingang der zweiten Logikschaltung 12 anliegt, die den DAS auf das Ausgangssignal anwendet, um Daten für eine Signatur zu erzeugen. Die beiden Logikschaltungen 21 und 22 und der Umschalter 24 bilden eine host-gesteuerte Cryptologik 20, welche einen Steuerdateneingang c aufweist und mit ihrem Ausgang d mit dem Informationseingang i des PSD 10 verbunden ist.

Die im IBI-Programm der amerikanischen Postbehörde USPS angegebenen nutzbaren Algorithmen sind RSA (Rivest, Shamir, Adleman), DAS (Digital Signature Algorithm), und ECDSA (Elliptic Curve Digital Signature Algorithm), welche jeweils mit dem SHA-1 (Secure Hash Algorithm) beschränkt werden.

Unter der Voraussetzung, dass ein Signierschlüssel sk eines postalischen Sicherheitsgerätes (PSD) auf eine Mitteilung m für einen ersten Zweck, beispielsweise zur Berechnung eines gewöhnlichen Freistempels (49 byte) angewendet wird, um die Signatur für die Mitteilung m wie folgt zu berechnen, ergibt sich:

$$sig = DSAsign(sk, SHA\text{-}1(m)) \quad (1)$$

Für einen zweiten Zweck sei die zweite Mitteilung M bestimmt. Im Unterschied zu der für einen ersten Zweck eingesetzte Gleichung (1) berechnet man die Signatur für einen zweiten Zweck, beispielsweise für einen Nachladefreistempel, wie folgt:

$$SIG = DSAsign(sk, SHA\text{-}1(SHA\text{-}1(M))) , \quad (2)$$

Durch die zweimalige Anwendung von SHA-1 statt einmaliger Anwendung von SHA-1 kann verhindert werden, dass eine für einen zweiten Zweck berechnete Signatur für einen ersten Zweck als zutreffend ausgegeben wird. Eine Sicherheitsbetrachtung zeigt, dass auf diese Weise ein betrügerischer Benutzer als Nebenprodukt eine gewöhnliche Signatur auf die Mitteilung:

$$m' = SHA\text{-}1(M) . \quad (3)$$

erhält, was zum Wiederverwenden nicht hilfreich ist, weil der Datensatz dieser Mitteilung eine Länge von 160 bit = 20 byte hat, während zum "Wiederverwenden" einer Signatur eine Mitteilung einen Datensatz mit einer Länge von 49 Byte aufweisen müsste. Praktisch ist das Bekanntsein irgendeines 49 Byte langen Datensatzes auch noch nicht für einen Betrug ausreichend. Damit der Betrug klappt, müsste der Betrüger den Datensatz schon zum grossen Teil selbst auswählen können.

Die Figur 3 zeigt eine Kombination gleicher Cryptoalgorithmen 221 und 222 innerhalb der Logikschaltung 22. Es ist vorgesehen, dass sich letztere durch die Anwendung eines anderen Cryptoalgorithmus oder durch die doppelte Anwendung des gleichen Cryptoalgorithmus von der Logikschaltung 21 unterscheidet.

Es gibt eine Vielzahl an anderen möglichen Kombinationen zur Bildung eines Cryptoalgorithmuses. Die Figur 4 zeigt einfache Strukturen solcher Cryptoalgorithmen, wobei sich die Logikschaltung 22 durch die zusätzliche Anwendung eines weiteren Cryptoalgorithmus von der Logikschaltung 21 unterscheidet. Es ist bekannt, einen HMAC zu bilden, der dabei auf einer bekannten Hashfunktion SHA-1 basiert. Ein H-MAC benötigt ausser der Nachricht m noch einen Schlüssel k als Eingabe. Es ist vorgesehen, dass sich letztere durch die zusätzliche Anwendung eines anderen Cryptoalgorithmus oder durch die Anwendung unterschiedlicher Schlüssel bei einem gleichen Cryptoalgorithmus von der Logikschaltung 21 unterscheidet. Man könnte als Schlüssel zwei öffentlich bekannte Parameter vereinbaren, zum Beispiel 1010 für gewöhnliche Freistempel und 0101 fuer Nachladefreistempel. Die Parameter müssen öffentlich bekannt sein, weil letztere der Empfänger der Freistempel ja ebenfalls zum Prüfen braucht. Bei dieser Variante tritt das Problem nicht auf, das in der obigen Sicherheitsbetrachtung genannten Einsatzfall zum Nachladefreistempel geschildert wurde, denn ein Nachladefreistempel wird zwar mit demselben Signierschlüssel, aber mit einer anderen Kombination von Signier- und Hash-Algorithmen gebildet, als gewöhnliche Freistempel. Ausserdem kann man ein Nachladen durch eine online Transaktion direkt mit der Hersteller-Infrastruktur durchführen, in einer analogen Weise zum Guthabennachladen. Zur Authentikation der entsprechenden Nachricht des PSD´s verwende man einen anderen Signierschlüssel als den für gewöhnliche Freistempel. Auf diese Weise können die entstehenden Signaturen niemals für Freistempelzwecke missbraucht werden.

In der Figur 5a ist eine zweite Variante einer host-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes dargestellt. Dabei wird ein

gewöhnliches postalisches Sicherheitsgerät PSD 10 mit einer Cryptologik 20 zusammengeschaltet und dabei dessen Funktionalität so erweitert, dass Signaturen entsprechend drei unterschiedlichen Zwecken gebildet werden können. Das gewöhnliche PSD 10 weist wieder zwei Logikschaltungen 11 und 12 auf, welche einen Software- oder Hardwaremodul beinhalten können. Die Cryptologik 20 verfügt einen host-gesteuerten eingangsseitigen Umschalter 24 für die Mitteilung m. Die Kontakte I, II und III des Umschalters 24 liegen jeweils am Eingang e1, e2, e3 einer der Logikschaltungen 11, 22, 23 an, wobei die Logikschaltungen 22 und 23 in der Cryptologik 20 angeordnet sind. Die Cryptologik 20 weist ausgangsseitig eine Zusammenschaltung der Ausgänge a2, a3 der Logikschaltung 22 und 23 und eine Verbindung des Ausgangs d zum Informationseingang i des PSD 10 auf. Der Ausgang a1 der Logikschaltung 11 ist ebenfalls mit dem Informationseingang i des PSD 10 verbunden. Der Informationseingang i des PSD 10 ist mit der zweiten Logikschaltung 12 eingangsseitig verbunden, die einen weiteren Algorithmus, beispielsweise einen DAS, auf das Ausgangssignal anwendet, um Daten für eine Signatur zu erzeugen.

Die Figur 5b zeigt eine PSD-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes nach einer ersten Variante. Das PSD hat eine interne Logikschaltung 11 für einen ersten Cryptoalgorithmus und eine zweite Logikschaltung 12, um die Daten für eine Signatur zu erzeugen. Die Cryptologik 20 weist Logikschaltungen für einen zweiten und dritten Cryptoalgorithmus 22 und 23 auf und benötigt keinen eingangsseitigen Umschalter. Dafür ist im PSD 10 ein PSD-gesteuerter eingangsseitiger Umschalter 14 für die Mitteilung m vorgesehen. Die Kontakte I, II und III des Umschalters 14 liegen jeweils am Eingang e1, e2, e3 einer der Logikschaltungen 11, 22, 23 an, wobei die Logikschaltungen 22 und 23 in der Cryptologik 20 angeordnet und zugehörige Eingänge e2 und e3 vorgesehen sind. Die Cryptologik 20 weist ausgangsseitig einen

Anschluss d zur Verbindung der Ausgänge a2, a3 der Logikschaltung 22 und 23 mit dem Informationseingang i des PSD 10 auf.

Die Figur 6 zeigt eine zweite Variante einer PSD-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes. Es ist kein eingangsseitiger Umschalter für die Mitteilung m vorgesehen, sondern letztere liegt am Eingang e_1 einer ersten Logikschaltung 21 für einen ersten Cryptoalgorithmus an. Deren Ausgang a_1 liegt am ersten Kontakt I eines Umschalter 14 innerhalb des PSD 10 an. Der Ausgang a_1 liegt außerdem am Eingang e_2 einer ersten Logikschaltung 11 im Inneren des PSD´s 10. Deren Ausgang a_2 liegt am zweiten Kontakt II des Umschalters 14 innerhalb des PSD 10 an. Beide jeweils erste Logikschaltung 21 und 11 können den gleichen Cryptoalgorithmus aufweisen und werden von der Mitteilung nacheinander durchlaufen, wenn der Kontakt II des Umschalters 14 über einen Steuerdateneingang c durchdas PSD ausgewählt ist. Der Ausgang a_1 der ersten Logikschaltung 21 liegt außerdem am Eingang e_3 einer dritten Logikschaltung 23 der Cryptologik 20, d.h. extern vom PSD 10. Deren Ausgang a_3 liegt am dritten Kontakt III des Umschalters 14 innerhalb des PSD 10 an. Bei dieser zweiten Variante einer PSD-gesteuerten Umschaltung erfolgt die Umschaltung zwischen der ersten Logikschaltung 21 und der dritten Logikschaltung 23, die beide extern vom PSD 10 angeordnet sind, und der ersten Logikschaltung 11, die intern im PSD 10 angeordnet ist, unmittelbar vor dem Durchlaufen der zweiten Logikschaltung 12 die intern im PSD 10 angeordnet ist.

Die Figur 7 zeigt eine PSD-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes nach Variante 3. Eine erste Logikschaltung 21 für einen ersten Cryptoalgorithmus weist einen Eingang e_1 für eine Mitteilung m und einen Ausgang a_1 auf, der mit einem Eingang e_2 für eine zweite Logikschaltung 23 für einen zweiten Cryptoalgorithmus verbunden ist, wobei

deren Ausgang a_2 mit einem Eingang e_3 für eine dritte Logikschaltung 23 für einen dritten Cryptoalgorithmus verbunden ist, wobei deren Ausgang a_3 am Informationseingang i des postalischen Sicherheitsgerätes 10 anliegt. Die Cryptologik 20 ist ausgangsseitig mit dem postalischen Sicherheitsgerätes 10 verbunden, wobei der Ausgang a_1 der ersten Logikschaltung 21 an einem ersten Kontakt I, wobei der Ausgang a_2 der zweiten Logikschaltung 22 an einem zweiten Kontakt II und wobei der Ausgang a_3 der weiteren Logikschaltung 23 an einem dritten Kontakt III eines PSD-gesteuerten Umschalters 14 innerhalb des postalischen Sicherheitsgerätes 10 anliegt. Der Umschalter 14 ist ausgangsseitig an eine zweite Logikschaltung 12 innerhalb des postalischen Sicherheitsgerätes 10 gekoppelt, die die Signatur erzeugt.

Die Figur 8 zeigt eine dritte Variante einer host-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes. Eine extern vom postalischen Sicherheitsgerät 10 angeordnete Cryptologik 20 ist mindestens mit ihrem Ausgang d mit einem Informationseingang i des postalischen Sicherheitsgerätes 10 verbunden. Das postalische Sicherheitsgerät 10 weist intern eine Logikschaltung 12 auf, die einen digitalen Signaturalgorithmus auf das vom Ausgang d gelieferte Ausgangssignal anwendet, um Daten für eine Signatur zu erzeugen. Die Cryptologik 20 weist eine Anzahl an Logikschaltungen 21, 23 und einen Umschalter 26 auf, der einen Steuerdateneingang c_2 hat, zur Steuerung durch einen - nicht gezeigten - Host. Der Umschalter 26 ist mit der weiteren Logikschaltung 23 verbunden und schaltet einen Schlüssel k1, k2 für den weiteren Cryptoalgorithmus um. Eine erste Logikschaltung 21 für einen ersten Cryptoalgorithmus weist einen Eingang e_1 für eine Mitteilung m und einen Ausgang a_1 auf, der mit einem Eingang e_3 für eine weitere Logikschaltung 23 für einen weiteren Cryptoalgorithmus verbunden ist, wobei deren Ausgang a_3 am Informationseingang i der zweiten Logikschaltung 12 anliegt, die die Signatur erzeugt.

Die Figur 9 zeigt eine vierte Variante einer host-gesteuerten Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes. Zusätzlich zur Schaltung der dritten Variante, die einen ersten Umschalter 26 ausweist, der einen Schlüssel k1, k2 für den weiteren Cryptoalgorithmus der weiteren Logikschaltung 23 umschaltet, ist ein zweiter Umschalter 24 in der host-gesteuerten Cryptologik 20 vorgesehen, wobei Kontakte I und II des Umschalters 24 mit den Ausgängen a_1 und a_3 der ersten und dritten Logikschaltung 21 und 23 verbunden sind. Der Umschalter 24 bildet ausgangsseitig den Ausgang d, der mit dem Informationseingang i des des postalischen Sicherheitsgerätes 10 verbunden ist. Es ist vorgesehen, dass die Umschalter 24 und 26 über einen Steuerdateneingang c_1, c_2 durch einen Host (nicht gezeigt) gesteuert werden.

Die Figur 10 zeigt eine Host- und PSD-gesteuerte Umschaltung der Cryptoalgorithmen für eine Generierung einer Signatur mittels des postalischen Sicherheitsgerätes. Das postalische Sicherheitsgerät 10 weist mindestens eine Logikschaltung 11 und die Cryptologik 20 weist mindestens eine Logikschaltung 23 auf. Die Cryptologik 20 hat einen ersten host-gesteuerten Umschalter 26, der einen Schlüssel k1, k2 für den weiteren Cryptoalgorithmus der weiteren Logikschaltung 23 umschaltet. Zur Umschaltung zwischen den Ausgängen a_1 bzw. a_3 der ersten bzw. dritten Logikschaltung 11 und 23 ist ein zweiter PSD-gesteuerter Umschalter 14 in dem postalischen Sicherheitsgerät 10 vorgesehen, wobei Kontakte I bzw. II des Umschalters 14 mit den Ausgängen a_1 bzw. a_3 der ersten bzw. dritten Logikschaltung 11 und 23 verbunden sind.

Die Figur 11 zeigt eine Blockschaltung eines Hostgerätes. Das postalische Sicherheitsgerät 10 und die Cryptologik 20 sind mittels Schnittstellen i, d über einen host-internen BUS 37 betriebsmäßig verbunden. Eine Hardeware und Interfaceschaltung 13 des postalischen Sicherheitsgerätes 10 für die Schnittstelle i kann beispielsweise mit einer anwendungs-

spezifischen Schaltung (ASIC) realiesiert werden. Leztere ist zur Durchführung der vorgenannten kryptographischen Funktionen mit einer Datenverarbeitungseinheit 16 und mit nichtflüchtigen Speichern 15 zur Durchführung von weiteren Funktionen verbunden. Die Datenverarbeitungseinheit 16 weist einen Mikroprozessor (µP) mit Echtzeituhr (RTC), FLASH-Speicher und Arbeitsspeicher (SRAM) auf. Das Sicherheitsgerät 10 verfügt über interne Überwachungseinheiten 17 und 19 und einen internen BUS 19. Das Hostgerät 1 verfügt ebenfalls über einen nichtflüchtigen Speicher 35, Mikroprozessor 36, Festwertspeicher 33, Arbeitsspeicher 34 sowie über ein Modem 32, Tastatur 39 und Displaycontroller 38 mit Anzeigeeinheit (nicht gezeigt). Das Hostgerät 1 kann über eine Kommunikationsverbindung 2 mit einer entfernten Datenzentrale 5 verbunden werden. Die Datenzentrale 5 verfügt beispielsweise über ein Modem 52, einen Server 53 und eine Datenbank 54. Das Hostgerät 1 ist – in nicht gezeigter Weise – über eine Kommunikationsverbindung oder Schnittstelle mit einem weiteren Gerät, beispielsweise einer Druckvorrichtung, verbindbar.

Die Erfindung ist nicht auf die vorliegenden bzw. solche Ausführungsformen beschränkt, bei denen mindestens zwei verschiedene durch eine Authorität zugelassene Hash-Funktionen bei demselben Signieralgorithmus benutzt werden. Alternativ kann dieselbe Hashfunktion bei zwei verschiedenen zugelas-senen Signieralgorithmen benutzt werden. Die Cryptologik 20 ist dann ebenfalls mit dem PSD 10 verbunden. Die verschiedenen zugelassenen Signieralgorithmen und deren Umschaltung werden softwaremäßig vorge-nommen. Die Cryptologik 20 enthält nur eine Logikschaltung 21 für einen Cryptoalgorithmus, zum Beispiel eine bekannte Hash-Funktion.

Es ist eine Vielzahl von alternativen Kombinationen im Rahmen der Ansprüche denkbar, die unterschiedlich ausgeführt sind. So können offensichtlich weitere andere Ausführungen der Erfindung entwickelt bzw. eingesetzt werden, die vom gleichen Grundgedanken der Erfindung ausgehend, die von den anliegenden Ansprüchen umfaßt werden.

***

Zusammenfassung

Verfahren und Anordnung zur unterschiedlichen Erzeugung kryptographischer Sicherungen von Mitteilungen in einem Hostgerät, wobei zur kryptographischen Sicherung einer Mitteilung für einen ersten Zweck eine erste Signatur zur kryptographischen Sicherung einer Mitteilung für einen zweiten Zweck eine zweite Signatur eingesetzt wird, wobei sich die Signaturen in der Art ihrer Erzeugung unterscheiden. Eine Cryptologik (20) weist eine Anzahl an Logikschaltungen (21, 22, 23) und einen Umschalter (24, 26) auf und ist extern vom postalischen Sicherheitsgerät (10) angeordnet und mindestens mit ihrem Ausgang (d) mit einem Informationseingang (i) des postalischen Sicherheitsgerätes (10) verbunden, das eine Logikschaltung (12) aufweist, die einen digitalen Signaturalgorithmus auf das vom Ausgang (d) gelieferte Ausgangssignal anwendet, um Daten für eine Signatur zu erzeugen. Fig. 2

****

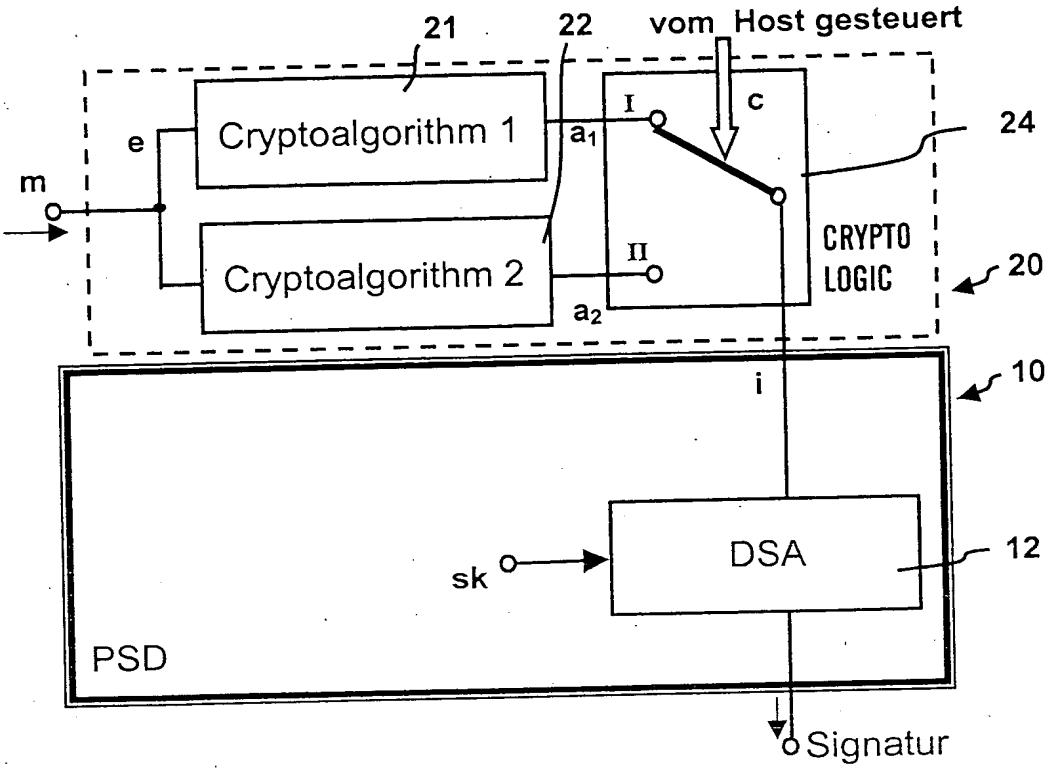

21
22
vom Host gesteuert
Cryptoalgorithm 1
Cryptoalgorithm 2
e
m
I
II
c
a_1
a_2
24
CRYPTO
LOGIC
20
10
i
sk
DSA
12
PSD
Signatur

Fig. 2

Patentansprüche:

1. Verfahren zur unterschiedlichen Erzeugung kryptographischer Sicherungen von Mitteilungen in einem Hostgerät, wobei zur kryptographischen Sicherung einer Mitteilung für einen ersten Zweck eine erste Signatur und zur kryptographischen Sicherung einer Mitteilung für einen zweiten Zweck eine zweite Signatur eingesetzt wird, gekennzeichnet dadurch, dass sich die Signaturen in der Art ihrer Erzeugung unterscheiden.

2. Verfahren nach Anspruch 1, gekennzeichnet dadurch, dass die kryptographischen Algorithmen zur Erzeugung von Signaturen programmgemäß im Festwertspeicher eines postalischen Sicherheitsgerätes (10), implementiert und dass die Signaturen programmgesteuert erzeugt werden, wobei mindestens ein kryptographischer Algorithmus hardwaremäßig und außerhalb des postalischen Sicherheitsgerätes (10) ausgeführt wird.

3. Verfahren nach Anspruch 1, gekennzeichnet dadurch, dass die kryptographischen Algorithmen zur Erzeugung von Signaturen programmgesteuert in separaten Logiken realisiert und Signaturen erzeugt werden.

4. Verfahren nach Anspruch 1, gekennzeichnet dadurch, dass eine beliebige Kombination von Signier- und Hash-algorithmen für einen Mitteilungstyp erzeugt wird, indem eine Logik allein oder in Verbindung mit Programmen im Festwertspeicher des postalischen Sicherheitsgerätes (10) und gegebenenfalls zusätzlich mit Programmen im Festwertspeicher des Hostgerätes mindestens einen bestimmten Algorithmus aus der Vielzahl der kryptographischen Algorithmen ausführt, wobei die Ausführung in Abhängigkeit vom einem jeweils eingestellten Mitteilungstyp gesteuert wird.

5. Anordnung zur unterschiedlichen Erzeugung kryptographischer Sicherungen von Mitteilungen in einem Hostgerät, mindestens mit einem postalischen Sicherheitsgerät (10), gekennzeichnet dadurch, dass eine Cryptologik (20) extern vom postalischen Sicherheitsgerät (10) angeordnet ist und mindestens mit ihrem Ausgang (d) mit einem Informationseingang (i) des postalischen Sicherheitsgerätes (10) verbunden ist und dass das postalische Sicherheitsgerät (10) eine Logikschaltung (12) aufweist, die einen digitalen Signaturalgorithmus auf das vom Ausgang (d) gelieferte Ausgangssignal anwendet, um Daten für eine Signatur zu erzeugen.

6. Anordnung, nach Anspruch 5, gekennzeichnet dadurch, dass eine host-gesteuerte Cryptologik (20) vorgesehen ist, welche einen Steuerdateneingang (c, c_1, c_2) aufweist.

7. Anordnung, nach den Ansprüchen 5 und 6, gekennzeichnet dadurch, dass die host-gesteuerte Cryptologik (20) eine Anzahl an Logikschaltungen (21, 22, 23) und einen Umschalter (24, 26) aufweist, der vom Host (1) gesteuert wird.

8. Anordnung, nach den Ansprüchen 5 bis 7, gekennzeichnet dadurch, dass eine erste Logikschaltung (21) für einen ersten Cryptoalgorithmus und eine zweite Logikschaltung (22) für einen zweiten Cryptoalgorithmus eingangsseitig verbunden sind und ausgangsseitig jeweils auf Kontakte (I und II) des Umschalters (24) führen, wobei letzterer ausgangsseitig am Eingang der zweiten Logikschaltung (12) anliegt, die die Signatur erzeugt. (Fig.2)

9. Anordnung, nach den Ansprüchen 5 bis 7, gekennzeichnet dadurch, dass das postalischen Sicherheitsgerät (10) eine erste Logikschaltung (11) für einen ersten Cryptoalgorithmus und eine zweite Logikschaltung (12) aufweist, die Daten für eine Signatur erzeugt, dass die host-gesteuerte Cryptologik (20) eine zweite und dritte Logikschaltung (22) und (23) und einen Umschalter (24) aufweist, wobei die erste Logikschaltung (11) des postalischen Sicherheitsgerätes (10) und die zweite und dritte Logikschaltung (22) und (23) ausgangsseitig mit dem Informationseingang (i) des postalischen Sicherheitsgerätes (10) verbunden sind, wobei der Informationseingang (i) mit der zweiten Logikschaltung (12) eingangsseitig verbunden ist, sowie dass der Umschalter (24) einen Eingang für eine Mitteilung (m) und Kontakte (I, II und III) aufweist, die jeweils am Eingang (e_1, e_2, e_3) der Logikschaltungen (11, 22, 23) anliegen. (Fig.5a)

10. Anordnung, nach den Ansprüchen 5 bis 7, gekennzeichnet dadurch, dass eine erste Logikschaltung (21) für einen ersten Cryptoalgorithmus einen Eingang (e_1) für eine Mitteilung (m) und einen Ausgang (a_1) aufweist, der mit einem Eingang (e_3) für eine weitere Logikschaltung (23) für einen weiteren Cryptoalgorithmus verbunden ist, wobei deren Ausgang (a_3) am Informationseingang (i) einer zweiten Logikschaltung (12) des postalischen Sicherheitsgerätes (10) anliegt, wobei die zweiten Logikschaltung (12) die Signatur erzeugt.

11. Anordnung, nach Anspruch 10, gekennzeichnet dadurch, dass mit der weiteren Logikschaltung (23) für den weiteren Cryptoalgorithmus ein Umschalter (26) verbunden ist, der einen Schlüssel (k1, k2) umschaltet. (Fig.8)

12. Anordnung, nach den Ansprüchen 10 bis 11, gekennzeichnet dadurch, dass ein erster und ein zweiter Umschalter (24, 26) in der host-gesteuerten Cryptologik (20) vorgesehen sind, wobei die Umschalter (24 und 26) über einen Steuerdateneingang (c_1, c_2) durch einen Host steuerbar sind, wobei Kontakte (I und II) des Umschalters (24) mit den Ausgängen (a_1) und (a_3) der ersten und dritten Logikschaltung (21) und (23) sowie dass der zweite Umschalter (24) ausgangsseitig den Ausgang (d) bildet, der mit dem Informationseingang (i) des postalischen Sicherheitsgerätes (10) verbunden ist. (Fig.9)

13. Anordnung, nach den Ansprüchen 5 und 6, gekennzeichnet dadurch, dass das postalische Sicherheitsgerät (10) und die Cryptologik (20) jeweils mindestens eine Logikschaltung (11) und (23) aufweisen und dass die Cryptologik (20) einen ersten host-gesteuerten Umschalter (26) aufweist, der einen Schlüssel (k1, k2) für den weiteren Cryptoalgorithmus der weiteren Logikschaltung (23) umschaltet, dass ein zweiter PSD-gesteuerter Umschalter (14) in dem postalischen Sicherheitsgerät (10) vorgesehen ist, wobei Kontakte (I bzw. II) des zweiten Umschalters (14) mit den Ausgängen (a_1 bzw. a_3) der ersten bzw. dritten Logikschaltung (11) und (23) verbunden sind. (Fig. 10)

14. Anordnung, nach Anspruch 5, gekennzeichnet dadurch, dass das postalische Sicherheitsgerät (10) oder die Cryptologik (20) mindestens eine Logikschaltung (11) und (22, 23) aufweisen sowie dass die Cryptologik (20) ausgangsseitig mindestens mit dem Ausgang (d) direkt oder indirekt auf den Eingang (i) der zweiten Logikschaltung (12) geschaltet ist, die im Inneren des postalischen Sicherheitsgerätes (10) angeordnet ist.

15. Anordnung, nach Anspruch 5, g e k e n n z e i c h n e t dadurch, dass das postalische Sicherheitsgerät (10) und die Cryptologik (20) jeweils mindestens eine Logikschaltung (11) und (22, 23) aufweisen sowie dass das postalische Sicherheitsgerät (10) einen PSD-gesteuerten Umschalter (14) mit einem Steuerdateneingang (c) aufweist, wobei die erste Logikschaltung (11) des postalischen Sicherheitsgerätes (10) und die zweite und dritte Logikschaltung (22) und (23) der Cryptologik (20) ausgangsseitig mit dem Informationseingang (i) des postalischen Sicherheitsgerätes (10) verbunden sind, sowie dass der Umschalter (14) einen Eingang für eine Mitteilung (m) und Kontakte (I, II und III) aufweist, die jeweils am Eingang (e_1, e_2, e_3) der Logikschaltungen (11, 22, 23) anliegen. (Fig.5b)

16. Anordnung, nach Anspruch 5, g e k e n n z e i c h n e t dadurch, dass eine erste Logikschaltung (21) für einen ersten Cryptoalgorithmus einen Eingang (e_1) für eine Mitteilung (m) und einen Ausgang (a_1) aufweist, der mit einem Eingang (e_3) für eine weitere Logikschaltung (23) für einen weiteren Cryptoalgorithmus verbunden ist, wobei deren Ausgang (a_3) am Informationseingang (i) des postalischen Sicherheitsgerätes (10) anliegt, dass die Cryptologik (20) ausgangsseitig mit dem postalischen Sicherheitsgerätes (10) verbunden ist, wobei der Ausgang (a_1) der ersten Logikschaltung (21) an einem ersten Kontakt (I) und wobei der Ausgang (a_3) der weiteren Logikschaltung (23) an einem dritten Kontakt (III) eines PSD-gesteuerten Umschalters (14) innerhalb des postalischen Sicherheitsgerätes (10) anliegt und wobei an einem zweiten Kontakt (II) des Umschalters (14) der Ausgang (a_2) einer ersten Logikschaltung (11) innerhalb des postalischen Sicherheitsgerätes (10) anliegt, welche eingangsseitig am Ausgang (a_1) der ersten Logikschaltung (21) der Cryptologik (20) angeschlossen ist und dass der Umschalter (14) ausgangsseitig an eine zweite Logikschaltung (12) innerhalb des postalischen Sicherheitsgerätes (10) gekoppelt ist, die die Signatur erzeugt.(Fig.6)

17. Anordnung, nach Anspruch 5, gekennzeichnet dadurch, dass eine erste Logikschaltung (21) für einen ersten Cryptoalgorithmus einen Eingang (e_1) für eine Mitteilung (m) und einen Ausgang (a_1) aufweist, der mit einem Eingang (e_2) für eine zweite Logikschaltung (23) für einen zweiten Cryptoalgorithmus verbunden ist, wobei deren Ausgang (a_2) mit einem Eingang (e_3) für eine dritte Logikschaltung (23) für einen dritten Cryptoalgorithmus verbunden ist, wobei deren Ausgang (a_3) am Informationseingang (i) des postalischen Sicherheitsgerätes (10) anliegt, dass die Cryptologik (20) ausgangsseitig mit dem postalischen Sicherheitsgerätes (10) verbunden ist, wobei der Ausgang (a_1) der ersten Logikschaltung (21) an einem ersten Kontakt (I), wobei der Ausgang (a_2) der zweiten Logikschaltung (22) an einem zweiten Kontakt (II) und wobei der Ausgang (a_3) der weiteren Logikschaltung (23) an einem dritten Kontakt (III) eines PSD-gesteuerten Umschalters (14) innerhalb des postalischen Sicherheitsgerätes (10) anliegt und dass der Umschalter (14) ausgangsseitig an eine zweite Logikschaltung (12) innerhalb des postalischen Sicherheitsgerätes (10) gekoppelt ist, die die Signatur erzeugt.(Fig.7)

*****

prior art

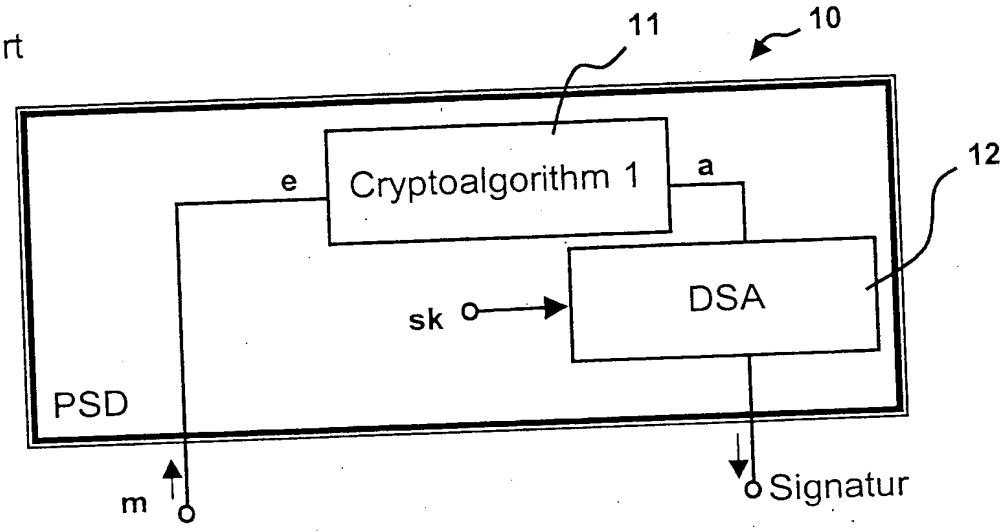


Fig.1

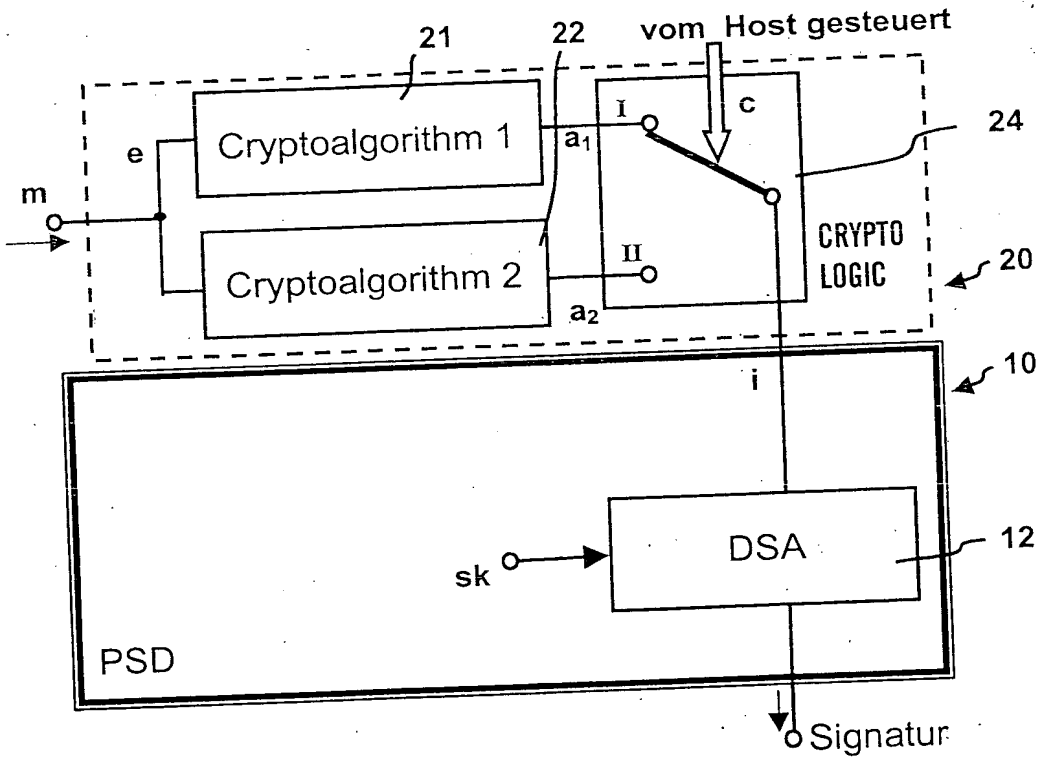


Fig. 2

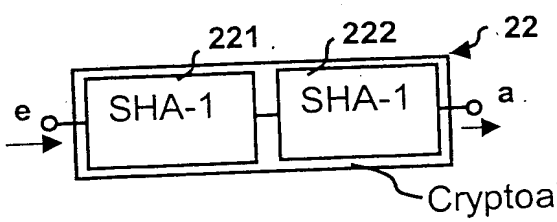


Fig. 3

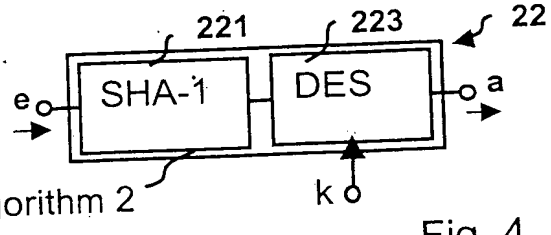


Fig. 4

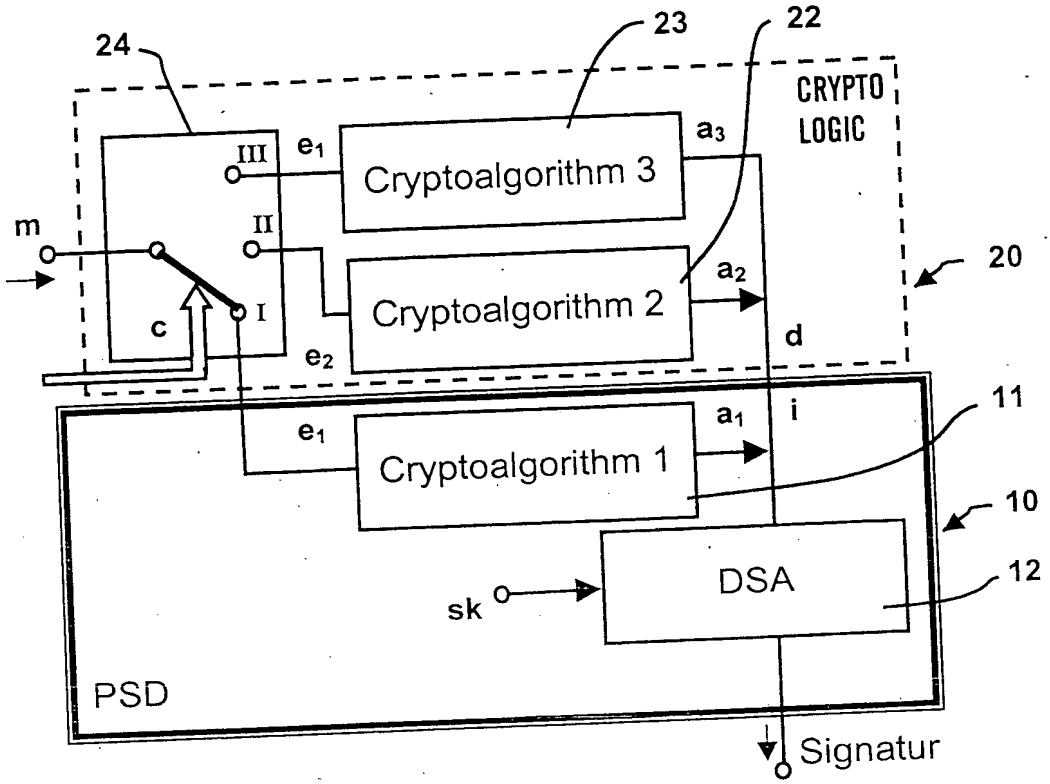

24
23
22
CRYPTO LOGIC
III
e1
Cryptoalgorithm 3
a3
m
II
Cryptoalgorithm 2
a2
20
c
I
e2
d
e1
a1
i
11
Cryptoalgorithm 1
10
DSA
12
sk
PSD
Signatur

Fig. 5a

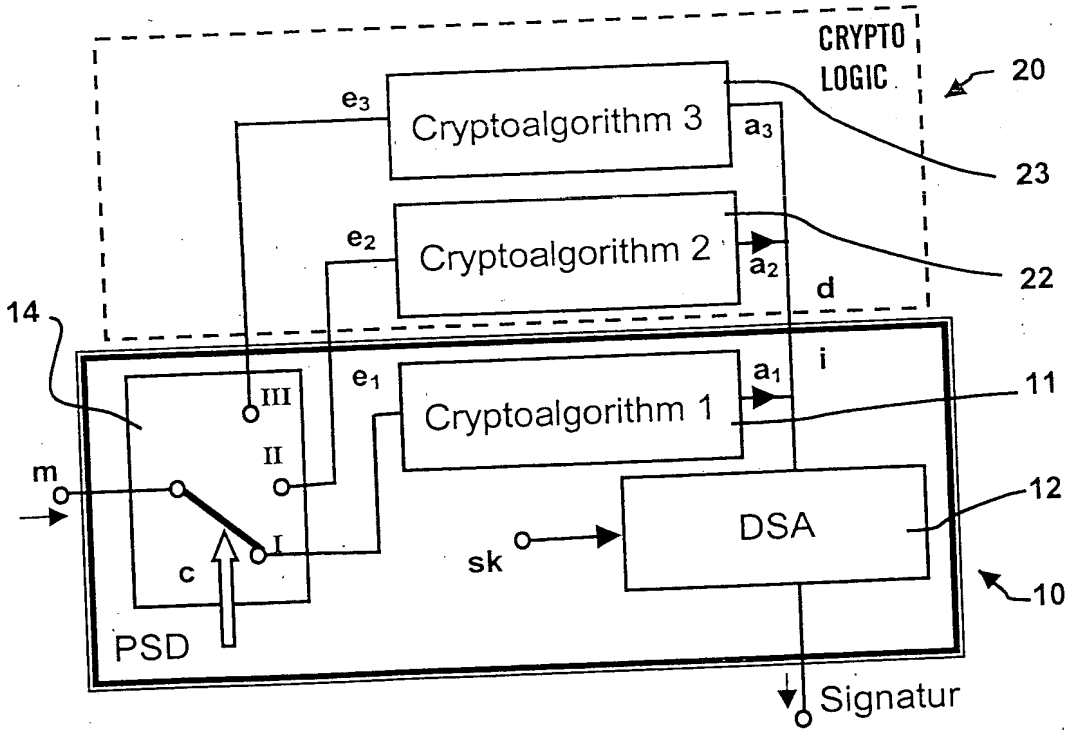
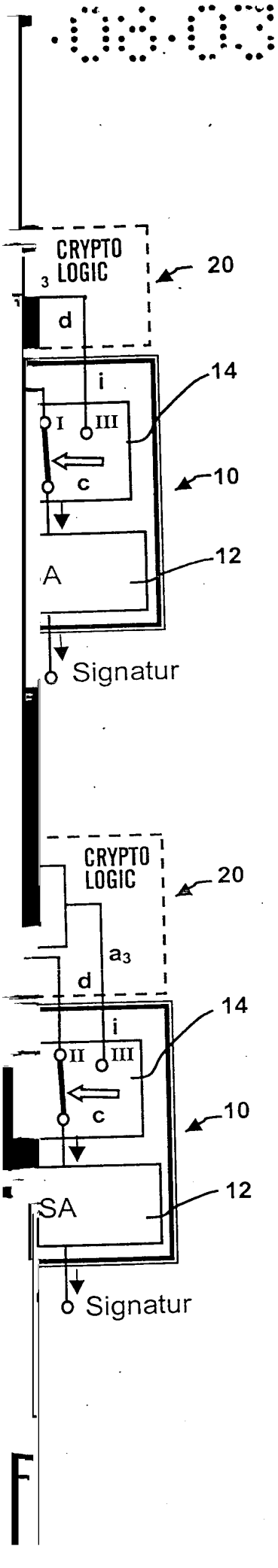

CRYPTO LOGIC
20
e3
Cryptoalgorithm 3
a3
23
e2
Cryptoalgorithm 2
a2
22
d
14
e1
a1
i
11
III
Cryptoalgorithm 1
II
m
12
DSA
I
sk
c
10
PSD
Signatur

Fig. 5b


CRYPTO LOGIC
3
d
20
i
14
I
III
c
10
A
12
Signatur
CRYPTO LOGIC
20
a3
d
i
14
II
III
c
10
SA
12
Signatur

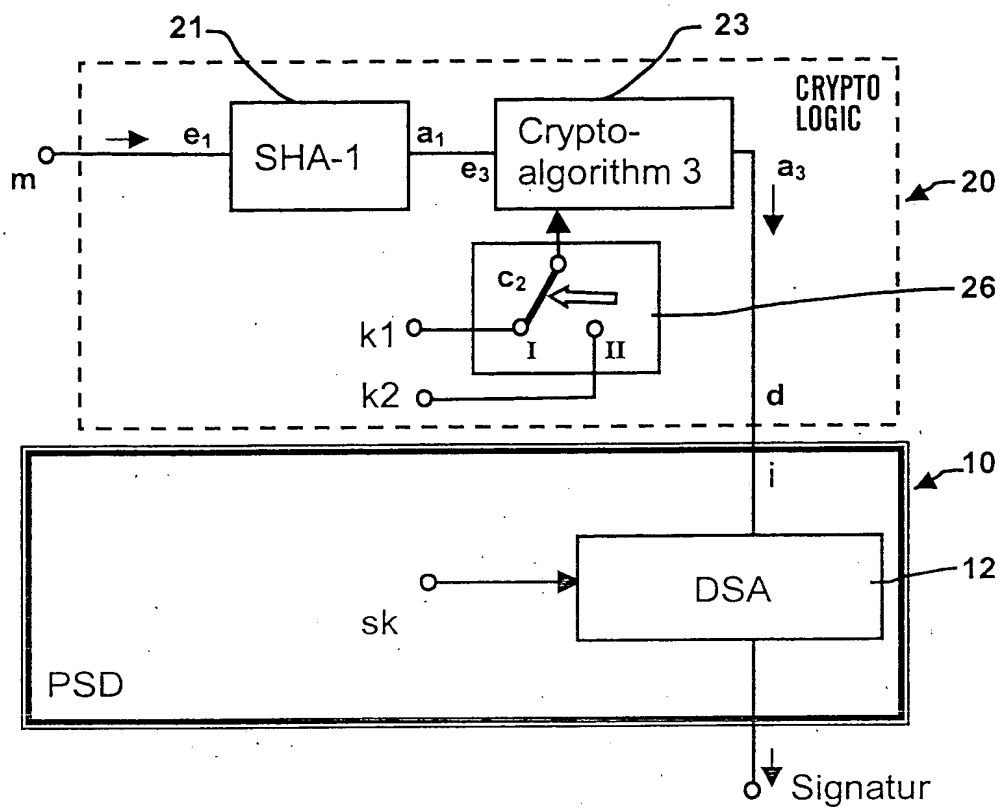

21
23
CRYPTO LOGIC
m
e1
SHA-1
a1
e3
Crypto-algorithm 3
a3
20
c2
26
k1
I
II
k2
d
10
i
DSA
12
sk
PSD
Signatur

Fig. 8

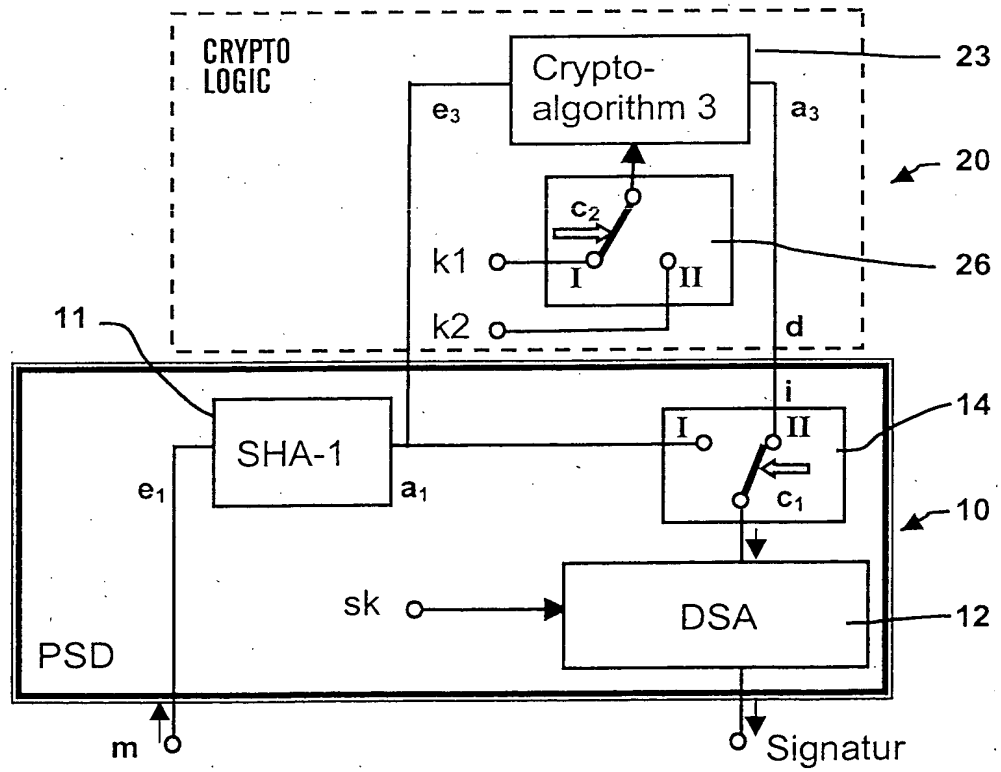

CRYPTO LOGIC
Crypto-algorithm 3
23
e3
a3
20
c2
k1
I
II
26
k2
d
11
i
14
SHA-1
e1
a1
c1
10
sk
DSA
12
PSD
m
Signatur

Fig. 10

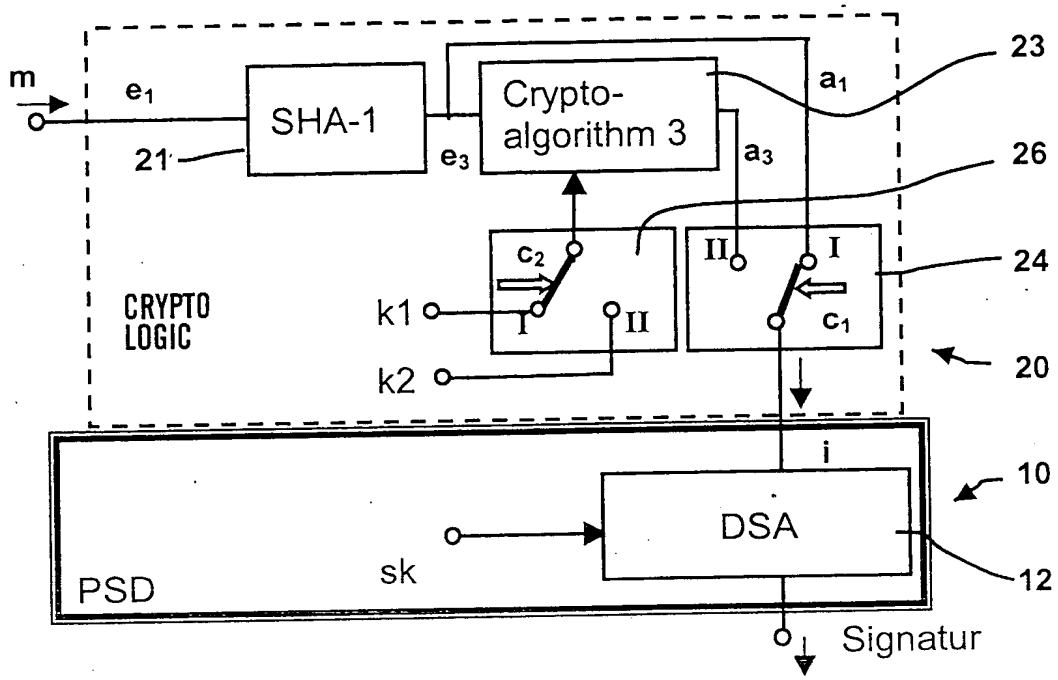

m
e1
21
SHA-1
e3
Crypto-
algorithm 3
a1
a3
23
26
24
c2
II
I
k1
I
II
k2
c1
CRYPTO
LOGIC
20
i
10
DSA
sk
12
PSD
Signatur

Fig. 9

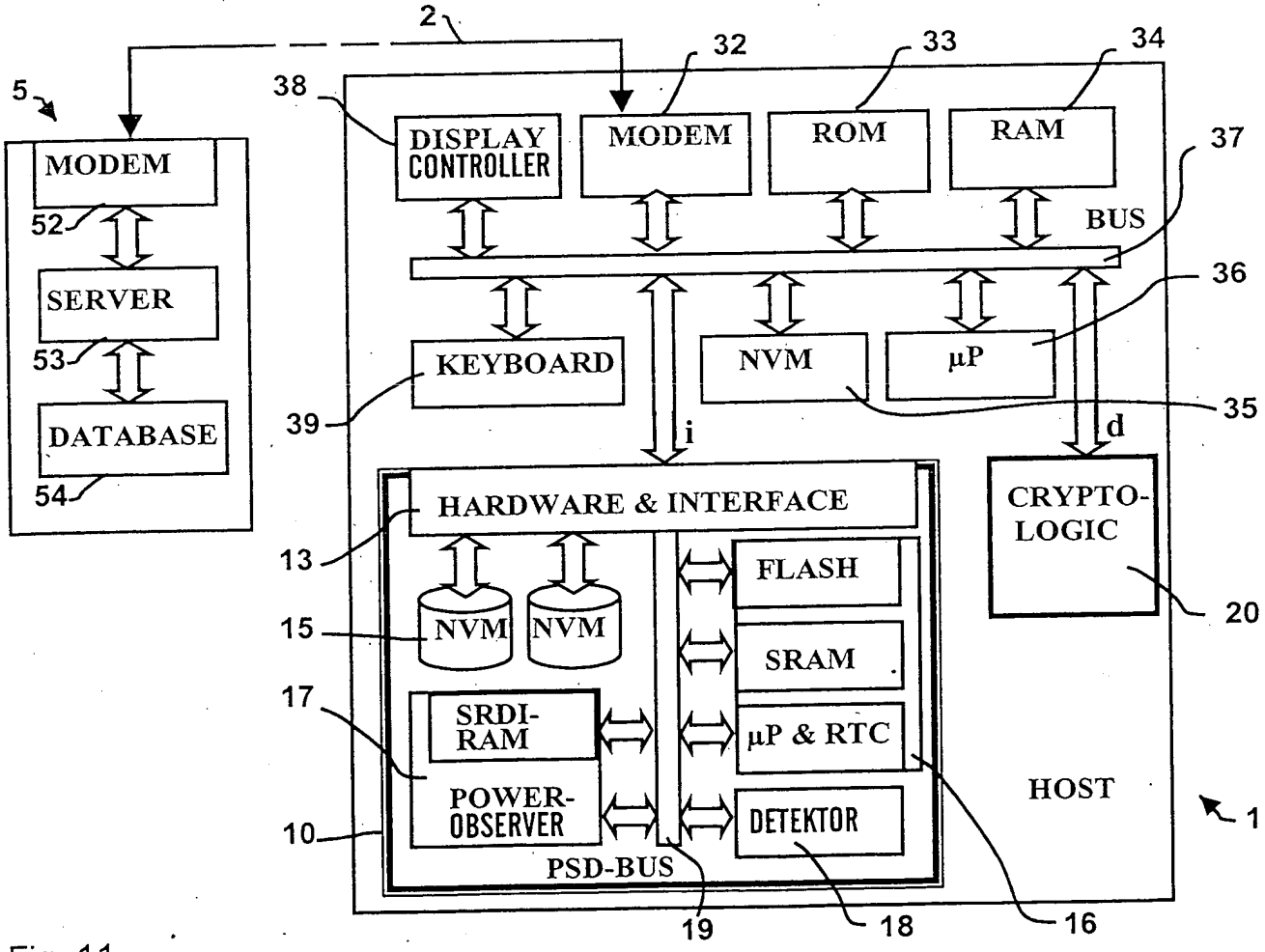

2
5
MODEM
52
SERVER
53
DATABASE
54
38
32
33
34
DISPLAY
CONTROLLER
MODEM
ROM
RAM
37
BUS
36
KEYBOARD
NVM
µP
39
35
i
d
HARDWARE & INTERFACE
13
FLASH
CRYPTO-
LOGIC
20
NVM
NVM
15
SRAM
17
SRDI-
RAM
µP & RTC
HOST
1
POWER-
OBSERVER
DETEKTOR
10
PSD-BUS
19
18
16

Fig. 11